



Octopus Conference on Cybercrime, Strasbourg, 11-13 July 2018


Workshop 1 – Evidence and jurisdiction in cyberspace: multi-stakeholder consultation on the Protocol to the Budapest Convention

- Context: Rationale for the Protocol – Recap and recent developments
- Provisions for more efficient mutual legal assistance
- Direct cooperation with providers across jurisdictions: Voluntary – Mandatory
- Access to data in the cloud/“transborder access” to data
- Next steps and further consultations



www.coe.int/cybercrime

Chatham House Rules apply



Context: Rationale for the Protocol – Recap and recent developments

About the Protocol to the Budapest Convention

- Being prepared by the Cybercrime Convention Committee (T-CY)
 - Protocol Drafting Group
 - Protocol Drafting Plenary
 - Sep 2017 – Dec 2019
- Elements under consideration
 - Provisions for more efficient MLA
 - Direct cooperation with providers in other jurisdictions
 - Framework for practices on extended searches/“transborder access”
 - Safeguards



Context: Rationale for the Protocol – Recap and recent developments

Setting the scene

- **Reach of Budapest Convention ► consider requirements of all Parties**
- **Challenges of criminal justice access to data in the cloud**
 - **Cloud computing: distributed systems ► distributed data ► distributed evidence**
 - **Unclear where data is stored and/or which legal regime applies**
 - **Service provider under different layers of jurisdiction**
 - **Unclear which provider for which services controls which data**
 - **Is data stored or in transit ► production orders, search/seizure or interception?**



Context: Rationale for the Protocol – Recap and recent developments

Setting the scene

- **Criminal justice scope of the Protocol ► Specific criminal investigations on cybercrime and e-evidence (article 14 and 25.1 Budapest Convention)**
- **Specific issues to be considered in Protocol**
 - **Differentiating subscriber versus traffic versus content data**
 - **Limited effectiveness of MLA**
 - **Loss of (knowledge of) location and transborder access jungle**
 - **Provider present or offering a service in the territory of a Party**
 - **Voluntary disclosure by US-providers**
 - **Emergency procedures**
 - **Data protection**



Context: Rationale for the Protocol – Recap and recent developments

Relevant international developments

- Location of data **versus** location of data controller or of person in possession or control
- US CLOUD Act
- EU e-evidence proposals:
 - Regulation on European Production and Preservation Orders
 - Directive on legal representatives

Question (a) : What are the implications of these developments for work on the Protocol?



Provisions for more efficient MLA

T-CY Recommendations 2014 and follow up given

<ul style="list-style-type: none"> ▪ T-CY assessment 2012-2014 ► Recommendations on <ul style="list-style-type: none"> • Monitoring efficiency of MLA • Training and allocation of staff and central and local levels • Strengthen 24/7 points of contact • Streamline procedures • Parallel domestic investigations • Etc. 	Domestic measures
<ul style="list-style-type: none"> • Emergency procedures • Language of requests • Joint investigations and joint investigation teams • Direct cooperation with providers • Expedited disclosure of subscriber information 	Via protocol



Provisions for more efficient MLA

T-CY Recommendations 2014 and follow up given

► Report on follow up given to RECs adopted by T-CY in November 2017

Mutual legal assistance is and will remain the primary means for obtaining electronic evidence for use in criminal proceedings. While additional solutions are being pursued to address situations where MLA is not feasible, States need to undertake the necessary efforts to render MLA more efficient in situations where MLA is feasible.

Information received shows that follow-up has been given by many States to many of the Recommendations. Good practices are available with respect to all Recommendations as inspiration to other States.



Provisions for more efficient MLA

Information and exchange of views on:

- **Emergency mutual legal assistance**
 - **Language of requests**
 - **Video conferencing**
-



Provisions for more efficient MLA

Emergency Mutual Assistance

- 1 ... an emergency means a situation in which there is a significant and imminent risk to the life or safety of any natural person.**
 - 2... each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists...**
 - 3 ... a requested Party shall accept such request in electronic form... Security and authentication....**
-



Provisions for more efficient MLA

Emergency Mutual Assistance

- 5 ... Once satisfied that an emergency exists and the other requirements for mutual assistance are satisfied, the requested Party shall respond to the request on the most rapidly expedited basis possible.**
- 6 ... Each Party shall ensure that a person from its authority responsible for responding to MLA requests is available 24/7.**
- 7 ... may agree to send advance copies or use alternate channels to respond.**

.....

Provisions for more efficient MLA

Languages of requests

Requests to a Party shall be made in a language acceptable to the requested Party or accompanied by a translation into such a language.

Note:

- While it is difficult to mandate a specific language in the Protocol, this provision is to permit flexibility in practice to speed up cooperation.
- T-CY to carry out informal surveys on acceptable languages.

Provisions for more efficient MLA

Video conferencing

Articles 9 and 10 of
2nd Additional
Protocol on MLA in
criminal matters >
detailed provisions



Article 18, para 18
of UN Convention
on Transnational
Organised Crime >
general provision

- ▶ Working on solution that is sufficiently specific to be effective and meet different requirements at the same time.



Provisions for more efficient MLA

Information and exchange of views on:

- Emergency mutual legal assistance
- Language of requests
- Video conferencing

Question (b) : Would civil society, data protection or industry organisations have any comments on such proposals?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Current practices:

- More than 170,000 requests/year by BC Parties/Observers to major US providers
 - Disclosure of subscriber information (ca. 64%)
 - Providers decide whether to respond to lawful requests and to notify customers
 - Provider policies/practices volatile
 - Data protection concerns
 - No disclosure by European providers
 - No admissibility of data received in some States
- Clearer / more stable framework required

Direct cooperation with providers across jurisdictions

<i>Parties and Observers (70 States)</i>	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
	Received	Disclosure	%
Albania	27	14	53%
Argentina	4 979	3 636	73%
Australia	6 555	4 543	69%
Belgium	2 521	2 301	91%
Canada	1 928	1 567	81%
Chile	1 488	1 094	74%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Italy	9 736	5 521	57%
Japan	3 822	2 598	68%
Netherlands	3 338	2 773	83%
Portugal	3 569	2 394	67%
Spain	6 353	3 418	54%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%

Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

► Scope and limitation of article 18 BC:

Guidance Note on Article 18 Budapest Convention on production of subscriber information

- **Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)**
- **Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)**



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (c): Can current practices by US providers be generalised in a Protocol?

- i. With regard to subscriber information?
- ii. For disclosure of other data in emergency situations?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (d) : What rules/regulations or other factors prevent providers from voluntarily disclosing subscriber information to criminal justice authorities from other jurisdictions?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Questions (e): Connecting factors: in what circumstances may service providers be subject to a domestic production order?

- i. “Real and substantial connection” to a Party?
- ii. Offering a service in the territory of a Party?
- iii. Or otherwise “established” in the Party?



Direct cooperation with providers across jurisdictions

About “offering a service”, “to be established“

CJEU: Google Spain versus Costeja

► Question of the territorial application of EU Directive 95/46:

“Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine **sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.”**



Direct cooperation with providers across jurisdictions

About “offering a service”, “to be established“

CJEU: Weltimmo (C-230/14) October 2015

... this results in a **flexible definition of the concept of ‘establishment’**, which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, in order to establish whether a company, the data controller, has an establishment, within the meaning of Directive 95/46, in a Member State other than the Member State or third country where it is registered, both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.



Direct cooperation with providers across jurisdictions

T-CY Guidance Note on Article 18:

A Party considers that a service provider is “**offering its services in the territory of the Party**” when, for example:

- the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);

and

- the service provider has established a real and substantial connection to a Party. Relevant factors include the extent to which a service provider orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), makes use of the subscriber information (or associated traffic data) in the course of its activities, interacts with subscribers in the Party, and may otherwise be considered established in the territory of a Party.

Direct cooperation with providers across jurisdictions

EU draft Regulation on European Production Orders

Article 2 (4) 'offering services in the Union' means:

- (a) enabling legal or natural persons in one or more Member State(s) to use the services listed under (3) above; and
- (b) having a substantial connection to the Member State(s) referred to in point (a);

... in the absence of such an establishment, a substantial connection should be assessed on the basis of:

- the existence of a significant number of users in one or more Member States,
- or the targeting of activities towards one or more Member States ►
 - factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services ...
 - availability of an application ('app') in the relevant national app store ...
 - providing local advertising or advertising in the language used in that Member State ...
 - handling of customer relations

23

Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Questions (e): Connecting factors: in what circumstances may service providers be subject to a domestic production order?

- i. "Real and substantial connection" to a Party?
- ii. Offering a service in the territory of a Party?
- iii. Or otherwise "established" in the Party?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (f) regarding data protection and other safeguards for voluntary disclosure:

i. Which data protection and other safeguards apply:

- Legal framework of country of service provider?
- Legal framework of country of requesting criminal justice authority?
- Legal framework of country where data is stored?
- Legal framework of country of data subject? What if several countries are involved?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (f) regarding data protection and other safeguards for voluntary disclosure:

ii. On the part of the service provider as the data controller under European legal frameworks:

- What conditions precisely have to be met to permit disclosure and which are the applicable provisions of the [GDPR](#) or Convention 108?
- What would be considered a sufficient legal basis under the GDPR or Convention 108?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (f) regarding data protection and other safeguards for voluntary disclosure:

ii. On the part of the service provider as the data controller under European legal frameworks:

- What constitutes a “legitimate interest” (Article 6.1.(f) GDPR) of a service provider in this context?
- What are requirements for disclosure/transfers of subscriber information to “third countries”?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

GDPR Article 6 – Lawfulness of processing

1.Processing shall be lawful only if and to the extent that at least one of the following applies:

- (e) processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
- (f) processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Question (f) regarding data protection and other safeguards for voluntary disclosure:

ii. On the part of the service provider as the data controller under European legal frameworks:

- Would the derogations of Article 49 GDPR – such as Article 49.1 (d) – apply if data is required in a specific criminal investigation?
- What is the meaning of Article 48 GDPR? What link between Articles 48 and 49?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

GDPR Article 48 - Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

GDPR Article 49 - Derogations for specific situations

In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal

....

(d) the transfer is necessary for important reasons of public interest;

Questions (f) ii

- Would the derogations of Article 49 GDPR – such as Article 49.1 (d) – apply if data is required in a specific criminal investigation?
- What is the meaning of Article 48 GDPR? Link between Articles 48 and 49?



Direct cooperation with providers across jurisdictions

Voluntary disclosure [of subscriber information] by service providers

Convention 108+

Article 14 – Transborder data flows

1-3 Between Parties or appropriate level of data protection

4 Derogations

c. Prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society

Questions (f) ii

- Would the derogations of Article 14.4.c apply if data is required in a specific criminal investigation?



Direct cooperation with providers across jurisdictions

Voluntary preservation of data by service providers

Question (g): Can current practices by US-providers be generalised in a Protocol?



Direct cooperation with providers across jurisdictions

Mandatory production orders

Considering the European Commission proposals for a European Production and Preservation Order:

Question (h): Could such a mandatory regime be envisaged for non-EU countries?

- i. For what type of data? Subscriber information only?
- ii. What limitations and connecting factors?
- iii. Role of competent authorities in requested country?
- iv. Enforcement in case of non-compliance with order?
- v. Safeguards and data protection requirements?



Lawful access to data in the cloud

► Understanding jurisdiction: Connecting factors

Question (i): What may be relevant factors to determine jurisdiction to enforce:

- location of data?
- location of equipment in the territory of a State?
- access by a person in the territory of a State who has “possession or control” of data?

Question (j): What is “transborder”?



Lawful access to data in the cloud

► Article 32 Budapest Convention

Question (k): Is further clarification needed on the scope of Article 32?



Lawful access to data in the cloud

Article 32 Budapest Convention – Trans-border access to stored computer data with consent or where publicly available

A Party may, **without the authorisation of another Party:**

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, **if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.**



Lawful access to data in the cloud

Guidance Note on Article 32 (adopted December 2014)

General considerations: Article 32b is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14.

On the person who can provide access or disclose data: Service providers are unlikely to be able to consent validly and voluntarily to disclosure of their users' data under Article 32.

On the location of the person consenting to provide access or disclose data: The standard hypothesis is that the person providing access is physically located in the territory of the requesting Party. However, multiple situations are possible.



Lawful access to data in the cloud

Typical scenario:

- A suspected drug trafficker is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another Party, police may access the data under Article 32b.



Lawful access to data in the cloud

“Transborder access” or extending a search?

Article 19 Budapest Convention - Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

- a a computer system or part of it and computer data stored therein; and
- b a computer-data storage medium in which computer data may be stored in its territory.

2 Measures to ensure that where authorities search or similarly access a specific computer system or part of it ... and have grounds to believe that the data sought **is stored in another computer system or part of it in its territory**, and such data is lawfully accessible from or available to the initial system, the authorities shall be able **to expeditiously extend the search or similar accessing to the other system**.



Lawful access to data in the cloud

Question (I): What other scenarios could be envisaged?

- Scenarios?
- Risks?
- Conditions and safeguards?



Next steps

Next steps and further consultations:

Consultations proposed for

Monday, 26 September 2018, 14h00 – 18h00, Strasbourg
